Small Business Innovation Research/Small Business Tech Transfer

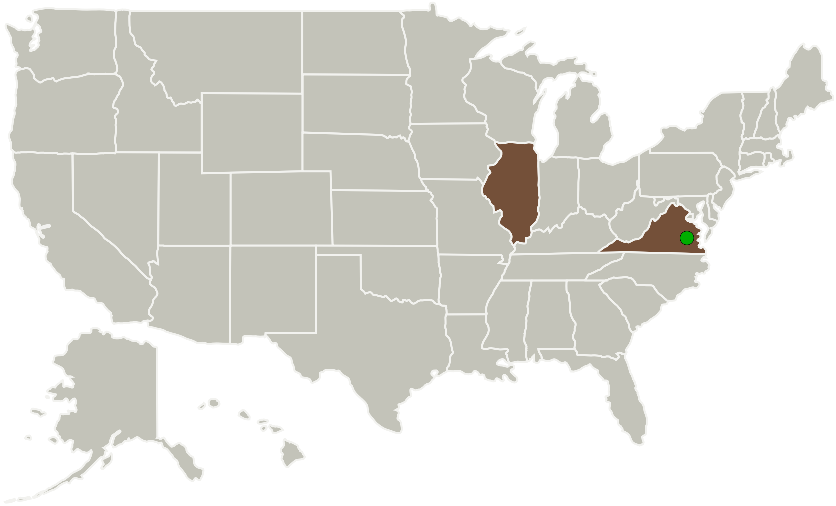
A Scalable Semantics-Based Verification System for Flight Critical Software, Phase II

Completed Technology Project (2014 - 2017)

Project Introduction

Flight-critical systems rely on an ever increasing amount of software—the Boeing 777 contains over 2 million lines of code. Most of this code is written in the C programming language. We need a scalable static formal program verification tool that is able to prove the functional correctness of flight-critical software, limiting any failure of flight critical software to hardware faults. This project seeks to leverage the matching logic verification framework. Matching logic is generic in an operational semantic of a given programming language, so we also seek to give a semantics of a subset of C, called CIL, which is guaranteed to be deterministic. While we already have a semantics for the entirety of C, CIL is more representative of flight-critical software, and the simpler, deterministic semantics will result in a more efficient, and thus more scalable, static program verification tool. We are also building a new unification- based rewrite engine that will result in a more powerful version of the Matching Logic Framework. In order to make the tool more commercially feasible, we will develop new techniques in pattern inference, so that loop invariants and some pre/post conditions can be determined automatically. We will perform a thorough evaluation of our tool on a large-scale piece of software with similar characteristics to a flight system.

Primary U.S. Work Locations and Key Partners



A Scalable Semantics-Based Verification System for Flight Critical Software, Phase II

Table of Contents

Organizations Performing Work	Role	Type	Location
Runtime Verification Inc	Lead Organization	Industry	Champaign, Illinois
🟢Langley Research Center(LaRC)	Supporting Organization	NASA Center	Hampton, Virginia

Primary U.S. Work Locations	
Illinois	Virginia

Project Transitions

▶ **April 2014:** Project Start

✓ **May 2017:** Closed out

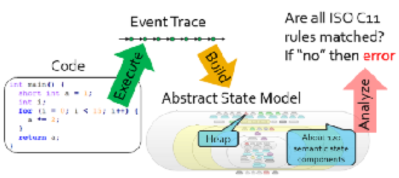
Closeout Summary: A Scalable Semantics-Based Verification System for Flight Critical Software, Phase II Project Image

Closeout Documentation:

- Final Summary Chart Image*(https://techport.nasa.gov/file/137621)*

Images

Briefing Chart Image
A Scalable Semantics-Based Verification System for Flight Critical Software, Phase II
(https://techport.nasa.gov/image/134256)



```
int main() {
  short int a = 1;
  int i;
  for (i = 0; i < 11; i++) {
    a += 2;
  }
  return a;
}
```

Event Trace
Are all ISO C11 rules matched? If "no" then error
Code
Execute
Build
Abstract State Model
Analyze
Heap
Abstract semantic state components

Final Summary Chart Image
A Scalable Semantics-Based Verification System for Flight Critical Software, Phase II Project Image
(https://techport.nasa.gov/image/126966)

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Organization:

Runtime Verification Inc

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Project Management

Program Director:

Jason L Kessler

Program Manager:

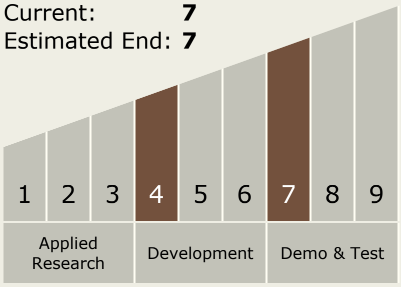
Carlos Torrez

Principal Investigator:

Dwight Guth

Technology Maturity (TRL)

Start:	**4**
Current:	**7**
Estimated End:	**7**



Technology Areas

Primary:

- TX04 Robotic Systems
  - └ TX04.6 Robotics Integration
    - └ TX04.6.3 Robot Software

Target Destinations

The Moon, Mars, Outside the Solar System, The Sun, Earth, Others Inside the Solar System